MASS. AF1.2: W38

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE FOR
ADMINISTRATION AND FINANCE
STATE HOUSE • ROOM 373
BOSTON, MA 02133

UMASS/AMHERST
312066 0278 0960 3

JANE SWIFT
GOVERNOR

STEPHEN P. CROSBY
SECRETARY

TEL: (617) 727-2040
FAX: (617) 727-2779

April 27, 2001

Re: Web Site Privacy Policy

To: Executive Department Secretariats, Agencies, and Authorities

I write to advise you of Governor Swift's Web site privacy policy. The Swift Administration believes strongly that the Commonwealth must do its utmost to protect the privacy of citizens who interact with the Executive Branch through its Web pages. It is critical that users have every opportunity to make fully informed decisions about the information they disclose when using our Web sites.

Accordingly, we are requiring each secretariat, agency, department, or other entity operating a Web site, to adopt, post, and enforce a suitable privacy policy. We have compiled baseline standards with which each of those Web page privacy policies must comply. I am enclosing a copy of these requirements with this letter.

The privacy policy in use at the Governor's Web site serves as a good model. However, we recognize that it may not be suitable for use by all agencies. You will need, therefore, to tailor your privacy policies to conform to laws and regulations that are specific to your agency.

Your privacy policy must be posted on your Web site no later than June 8, 2001. If you have a compelling need for additional time, please contact me in writing to request an extension.

As to independent authorities, we urge and encourage you to adopt policies that are in compliance with this directive.

Thank you for your cooperation in assisting us to achieve this important goal.

Very truly yours,

Stephen P. Crosby
Secretary

REQUIREMENTS FOR AGENCY WEB SITE PRIVACY POLICIES

Each agency must, by June 8, 2001, adopt, enforce and post on its Web site a privacy policy that complies with the following requirements. Each agency that operates a Web site must submit a copy of the privacy policy by e-mail to Linda Hamel, General Counsel for ITD, at Linda.Hamel@ITD.state.ma.us prior to June 1, 2001, for review prior to posting it. Agencies which have a compelling need for an extension of time for posting their privacy policy can seek such an extension by contacting the Secretary for Administration and Finance, Stephen P. Crosby, in writing to explain the unique circumstances that will prevent them from complying with this directive.

The privacy policy posted on the Governor's Web site is an example of a policy that, at least with respect to the Governor's Office, meets the requirements of this directive. However, note that the Governor's Office Web site policy does not include some of the information required below because the Governor's Office's Web site is not used for the same purposes, and is not governed by the same agency-specific laws and regulations, as state agencies. For instance, in comparison to other Commonwealth sites, the Governor's Web site does not collect information through the use of on-line forms and does not use "cookies". Agencies seeking to comply with this directive can use the Governor's Web site privacy policy as a model, but because it may not sufficiently address the requirements of this directive as it applies to their operations, must modify the policy as needed.

Location and Language.

A link for the Web site policy must be posted prominently on every page of every Executive Department Web site, and the policy itself must be written in clear, non-technical English accessible to the ordinary reader.

Information gathered at the Web site.

Cookies, logs and other automatic information gathering processes. No agency may commence using or continue to use "cookies" at their Web site without: (1) notifying ITD of the agency's intention to do so; (2) explaining the purposes for which the agency will use them; and (3) receiving ITD's written approval for such use. All agencies currently using "cookies" must file a written request for approval to ITD by May 18, 2001. In general, the Administration discourages the use of cookies. Agencies should consult with their Chief Information Officer or Director of Internet Services Sarah Bourne at Sarah.Bourne@itd.state.ma.us if they have questions about whether cookies are used on their Web pages and, if so, what kind.

Each Web site privacy policy must describe, in layperson's terms, all automatic information gathering processes, such as cookies, security logs, and other methods, used by the site. The user must be provided with information about the type of automatic information gathering processes used (including, where

necessary, the type of cookies used), how the agency uses the information, and how long the agency keeps the records created through such processes. Note that all agencies must comply with the Records Retention Law, M.G.L. c. 66, sec. 8, in determining how long they will retain such records.

Forms, E-mail and other voluntary information gathering processes. The policy must describe all means by which the site collects voluntary information from users, including click-throughs, forms, and e-mails. The policy must state whether voluntarily collected information will include personally identifiable information.

Uses of personally identifiable information gathered at the site.

Personally identifiable information is any information that could reasonably be used to identify a user personally, including his or her name, address, e-mail address, Social Security number, birth date, bank account information, credit card information, or any combination of information that could be used to identify the user. The term "personally identifiable information" should be used and defined in the policy.

The policy must describe how the agency uses personally identifiable information obtained by it through the site.

Dissemination of personally identifiable information.

The policy cannot include any "guarantees" of privacy. Rather, it must specifically state that personally identifiable information collected at the site may be subject to disclosure to members of the general public under the Public Records Law, M.G. L. c. 66, sec. 10. In addition, the policy must identify those to whom the agency will provide such information, and state that only Commonwealth employees with a "need to know" will have access to it. The policy must also state that the agency complies with the Fair Information Practices Act, M.G.L. c. 66A, and Executive Order 412 with respect to all personally identifiable information collected at the site.

While all Executive Department agencies are subject to the foregoing laws and Executive Order, state agencies administer and are subject to additional state laws pertaining to privacy and confidentiality. Therefore, each privacy policy must also refer to (and give a citation for) the special privacy or confidentiality laws or regulations to which the agency is subject with respect to information collected by it at the Web site.

Web sites directed at or knowingly collecting information from children.

State agencies operating Web sites or pages directed at children (age twelve or below), or knowingly collecting information from children on-line, must comply with the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. sec. 6501 et seq., to the extent possible for a government agency. Agencies wishing to operate Web sites directed to children should consult with ITD prior to posting such material.

Privacy policies for such sites or pages must state the special privacy protections built into the site for the purpose of complying with the terms of this law.

Review and correction of personally identifiable information.

Each privacy policy must state how users can review and correct personally identifiable information about them obtained by the Commonwealth through the Web site. Agencies are reminded that any method described in such a provision must be consistent with the Public Records Law, the Fair Information Practices Act, and the Records Retention Law.

Security.

The privacy policy must state what security procedures, if any, the agency provides in connection with communications between the user and the Web site.

Legal Review.

Before being posted, each agency Web site privacy policy must be reviewed by agency counsel. Agency counsel must report to the agency head whether the agency's use of the Web site and the information collected through it complies with the Public Records Law, the Records Retention Law, the Fair Information Practices Act, COPPA (to the extent possible for a public agency) and Executive Order 412. In addition, agency counsel must report whether the agency's use of the Web site and the information collected through it complies with any special laws restricting the agency's use of personally identifiable information. Agencies whose use of information in connection with a Web site does not comply with these laws and the Executive Order must immediately rectify such errors prior to posting the privacy policy on the Web site.

Contact person.

Each privacy policy must identify a contact person at the agency who will handle questions and complaints about on-line privacy matters.

Policy changes.

Each privacy policy shall state the terms under which the policy can be changed, including the number of days notice that users will have with respect to such changes.

Distribution of agency web site privacy policy.

Each agency must provide a copy of its Web site privacy policy to each new agency employee at the time of hire, to each current agency employee within a week of the agency's adoption of the policy, and to each vendor who services the Web site at the

time that the agency enters an engagement with the vendor, and must ensure that such parties uphold the terms of the privacy policy.

Further Information.

If you have questions about any of the matters referred to in this directive, please contact Linda Hamel at (617)-626-4404 or Linda.Hamel@itd.state.ma.us.